

# Unique Decoding of Plane AG Codes via Interpolation

Kwankyu Lee, Maria Bras-Amorós, and Michael E. O’Sullivan

## Abstract

We present a unique decoding algorithm of algebraic geometry codes on plane curves, Hermitian codes in particular, from an interpolation point of view. The algorithm successfully corrects errors of weight up to half of the order bound on the minimum distance of the AG code. The decoding algorithm is the first to combine some features of the interpolation based list decoding with the performance of the syndrome decoding with majority voting scheme. The regular structure of the algorithm allows a straightforward parallel implementation.

## Index Terms

Algebraic geometry codes, interpolation decoding, Gröbner bases.

## I. INTRODUCTION

Unique decoding of algebraic geometry codes is now a classical subject. By the works of Justesen et al., Skorobogatov and Vlăduț, and many others, the paradigm of decoding via syndromes using error locator polynomials and evaluator polynomials is well established [1]. Enhanced by Feng and Rao’s majority voting, the syndrome decoding algorithm for AG codes is capable of correcting errors up to half of the Feng-Rao bound, also called the order bound, which is no less than the designed distance. Until the advent of Guruswami and Sudan’s list decoding algorithm based on interpolation [2], the syndrome decoding algorithm had long been a uniquely available algorithm for decoding AG codes. Since then, the superiority in decoding performance of the list decoding algorithm has somewhat faded the syndrome decoding algorithm.

The superior performance of the list decoding is gained at the expense of large computational complexity. Table I below, excerpted from [3], shows an experimental result about the performance of the list decoding algorithm for the Hermitian code of length 27 and dimension 14. Here  $\tau$  denotes the number of errors that the list decoder is guaranteed to correct with multiplicity parameter  $m$ , and the number of successful decodings was counted out of 10,000 random error vectors of weight  $t$ . The notation  $\infty$  is used when successful decoding is guaranteed, as  $t \leq \tau$ . We may compare the result with the decoding performance of the syndrome decoding algorithm, which can correct errors of weight half of the designed distance, that is, 5 in this case. The list decoding algorithm certainly has better performance because, with multiplicity parameter 25, it can decode up to 6 errors, though the increased complexity is prohibitively high.

Moreover note that, to match the performance of the syndrome decoding algorithm, that is, to be guaranteed for successful decoding up to 5 errors, the multiplicity parameter should be at least 5. This means, for the same performance, the list decoding algorithm suffers slow decoding speed. On the other hand, observe from the experiment that list decoding with multiplicity  $m = 1$  performs almost as well as syndrome decoding. It corrects most cases of 5 errors, but unfortunately misses some. Since successful decoding only up to 2 errors is guaranteed by the theory of list decoding, this is a much better performance than expected.

Beside the performance, the two kinds of decoding algorithms, one based on interpolation and the other on syndromes, have different features. The list decoding algorithm decodes in the primal AG code, whose codeword

K. Lee is with the Department of Mathematics, Chosun University, Gwangju 501-759, Korea (e-mail: kwankyu@chosun.ac.kr). His work is supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2009-0064770) and also by research fund from Chosun University, 2008.

M. Bras-Amorós is with the Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Tarragona 43007, Catalonia, Spain (e-mail: maria.bras@urv.cat). Her work is supported by the Spanish Government through the projects TIN2009-11689 “RIPUP” and CSD2007-00004 “ARES”.

M. E. O’Sullivan is with the Department of Mathematics and Statistics, San Diego State University, San Diego, CA 92182-7720, USA (e-mail: mosulliv@math.sdsu.edu). His work is supported by the National Science Foundation under Grant No. CCF-0916492.

$m$	$\tau$	$t$							
		2	3	4	5	6	7	8	9
1	2	$\infty$	10000	10000	9977	998	85	2	0
2	3	$\infty$	$\infty$	10000	10000	282	1	0	0
3	4	$\infty$	$\infty$	$\infty$	10000	109	0	0	0
5	5	$\infty$	$\infty$	$\infty$	$\infty$	1119	0	0	0
25	6	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$			

TABLE I

is obtained by evaluation at rational points of the base curve, while the syndrome decoding algorithm decodes in the dual code. The former computes the message directly from the so-called  $Q$ -polynomial, while the latter obtains the message after computing the error locations and the error values from the error locator and evaluator polynomials. Finally, the syndrome decoding algorithm is equipped with the majority-voting scheme while there is no corresponding mechanism for list decoding.

These observations lead to the view, already widely accepted to experts in this area, that the list decoder with multiplicity one is closely related to the syndrome decoding algorithm without majority voting enhancement. However, they cannot be equivalent, principally due to the fact that one algorithm is for the primal code while the other one is for the dual code. Hence there is a missing idea corresponding to the majority voting in the context of interpolation based decoding, to match up the performance of the syndrome decoding algorithm. In this paper, we present an interpolation based unique decoding algorithm capable of correcting up to half of the order bound. The algorithm is an amalgamation of the decoding algorithm with multiplicity one and list size one in [3] and a recursion procedure that resembles the majority voting of Duursma [4]. Like list decoding, our unique decoding algorithm decodes in the primal codes and computes the message directly from the received vector. Like Kötter's algorithm [5], it allows an efficient parallel implementation.

In Section II, we review basic concepts and establish notations regarding AG codes on plane algebraic curves. We refer the reader to [6], [7], [8] for the basic theory of algebraic curves and AG codes over finite fields, and [9], [10] for Gröbner bases and commutative algebra. In Section III, we present and prove a unique decoding algorithm, using a majority voting procedure as a fundamental decoding method. In Section IV, we give a decoding example of Hermitian codes. In Section V, we conclude with brief remarks.

## II. PRELIMINARIES

Let  $X$  be an irreducible plane curve defined by the equation  $E(x, y) = 0$  over a field  $\mathbb{F}$  where

$$E(x, y) = y^a + \sum_{ai+bj < ab} c_{i,j} x^i y^j + cx^b$$

with  $\gcd(a, b) = 1$  and  $0 \neq c \in \mathbb{F}$ . These curves are known as Miura-Kamiya curves in the literature [11]. It is well known that  $X$  has a unique point  $P_\infty$  at infinity that is either nonsingular or a cusp. Hence there is a unique valuation  $v_{P_\infty}$  associated with  $P_\infty$ . Let  $\delta(f) = -v_{P_\infty}(f)$  for  $f$  in the coordinate ring  $R$  of  $X$ . Let  $\delta_x = \delta(x) = a$  and  $\delta_y = \delta(y) = b$ . By the equation of the curve, the ring  $R = \mathbb{F}[x, y]$  is a free module over  $\mathbb{F}[x]$  of rank  $a$  with basis  $\{y^j \mid 0 \leq j < a\}$ . The semigroup of  $R$  at  $P_\infty$

$$S = \{\delta(f) \mid f \in R\} = \{i\delta_x + j\delta_y \mid 0 \leq i, 0 \leq j < a\}$$

is a subset of the Weierstrass semigroup at  $P_\infty$ . For each nongap  $s \in S$ , there is a unique monomial  $x^i y^j \in R$  with  $0 \leq j < a$  such that  $\delta(x^i y^j) = s$ . Let us denote the monomial by  $\varphi_s$ .

Let  $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$  be a set of nonsingular affine rational points of  $X$  and let  $\mathbb{F}^n$  be the Hamming space over  $\mathbb{F}$ . The evaluation  $\text{ev} : R \rightarrow \mathbb{F}^n$  defined by  $\varphi \mapsto (\varphi(P_1), \varphi(P_2), \dots, \varphi(P_n))$  is a linear map over  $\mathbb{F}$ . Let  $u$  be a fixed positive integer less than  $n$  and define

$$L_u = \{f \in R \mid \delta(f) \leq u\} = \langle \varphi_s \in R \mid s \in S, s \leq u \rangle$$

where brackets denote the linear span over  $\mathbb{F}$ . Then the AG code  $C_u$  is defined as the image of  $L_u$  under  $\text{ev}$ . As  $u < n$ , the evaluation is one-to-one on  $L_u$ . Therefore the dimension  $k$  of the code  $C_u$  equals  $\dim_{\mathbb{F}} L_u$ , which equals

the size of the set  $\{s \in S \mid s \leq u\}$ . Let  $\{s \in S \mid s \leq u\} = \{s_1, s_2, \dots, s_k\}$ . By nonsystematic encoding, a message

$$m = (m_1, m_2, \dots, m_k) \in \mathbb{F}^k$$

is encoded to the codeword  $\text{ev}(\mu) \in C_u$  where

$$\mu = \sum_{i=1}^k m_i \varphi_{s_i} \in L_u.$$

For each  $1 \leq i \leq n$ , let  $\mathfrak{m}_i = \langle x - \alpha_i, y - \beta_i \rangle$  be the maximal ideal of  $R$  associated with the point  $P_i = (\alpha_i, \beta_i)$ . Then we have

$$\mathfrak{m}_i + \prod_{j \neq i} \mathfrak{m}_j = \langle 1 \rangle.$$

Therefore there exist  $g_i$  and  $h_i$  such that

$$g_i + h_i = 1, \quad g_i \in \mathfrak{m}_i, \quad h_i \in \prod_{j \neq i} \mathfrak{m}_j.$$

Then  $h_i(P_i) = 1$  and  $h_i(P_j) = 0$  for  $j \neq i$ . This set of  $h_i$  is called a *Lagrange basis* for the points  $P_1, \dots, P_n$ . A Lagrange basis can be easily computed as follows. Let  $t$  be the number of distinct  $x$ -coordinates of the points  $P_i$ . For each of these  $x$ -coordinates, there are at most  $a$   $y$ -coordinates of the points with the same  $x$ -coordinate. If  $h_{i,x} \in \mathbb{F}[x]$  and  $h_{i,y} \in \mathbb{F}[y]$  are polynomials such that  $h_{i,x}$  vanishes at the  $x$ -coordinates except that of  $P_i$  and  $h_{i,y}$  vanishes at the  $y$ -coordinates except that of  $P_i$ , then let

$$h_i = \frac{h_{i,x} h_{i,y}}{h_{i,x}(\alpha_i) h_{i,y}(\beta_i)} \in R$$

Note that  $\deg_x(h_{i,x} h_{i,y}) = t - 1$ . We assume  $h_i$  are precomputed prior to decoding.

As  $R$  is an  $\mathbb{F}[x]$ -module of rank  $a$  with free basis  $\{y^j \mid 0 \leq j < a\}$ , a polynomial in  $R[z]$  can be written as a unique  $\mathbb{F}$ -linear combination of the monomials in

$$\Omega = \{x^i y^j z^k \mid 0 \leq i, 0 \leq j < a, 0 \leq k\}.$$

For an integer  $s$ , we define the weighted degree of a monomial  $x^i y^j z^k \in \Omega$  by

$$\delta_s(x^i y^j z^k) = \delta(x^i y^j) + sk = \delta_x i + \delta_y j + sk.$$

Using  $\delta_s$ , we endow a weighted degree order  $>_s$  on  $\Omega$ , breaking ties in weighted degrees by  $z > y > x$ . Note that  $>_s$  restricted to the monomials belonging to  $Rz \oplus R$  is a monomial order for  $\mathbb{F}[x]$ -modules. The weighted degree order restricted to  $R$  is simply denoted by  $>_\delta$  as it is independent of  $s$ .

Note that  $Rz \oplus R$  is a free  $\mathbb{F}[x]$ -module of rank  $2a$  with a free basis  $G = \{y^j z, y^j \mid 0 \leq j < a\}$ . There is a simple criterion of a Gröbner basis of an  $\mathbb{F}[x]$ -submodule of  $Rz \oplus R$  with respect to any monomial order.

**Proposition 1.** *Let  $M$  be a submodule of  $Rz \oplus R$ , and let  $>$  be a monomial order on  $Rz \oplus R$ . Suppose  $B$  is a subset of  $M$  that generates  $M$ . If elements of  $B$  have leading terms that are  $\mathbb{F}[x]$ -multiples of distinct elements of  $G$ , then  $B$  is a Gröbner basis of  $M$  with respect to  $>$ . If this is the case,  $B$  is also a free basis of  $M$ .*

For a polynomial  $\varphi$ ,  $\text{lt}(\varphi)$  denotes the leading term with respect to a given monomial order, and  $\text{lc}(\varphi)$  denotes the coefficient of the leading term. Finally, for  $f \in \mathbb{F}[x]$  the bracket notation  $f[x^k]$  refers to the coefficient of the term  $x^k$  in  $f$ .

### III. INTERPOLATION DECODING

Let  $v$  be a received vector in  $\mathbb{F}^n$ . Let  $c \in C_u$  be such that  $v = e + c$ . Then there is a unique

$$\mu = \sum_{s \in S, s \leq u} \omega_s \varphi_s \in L_u$$

with  $c = \text{ev}(\mu)$ .

Let us denote the module of  $z$ -linear polynomials over  $R$  that interpolate the points  $(P_i, v_i)$  by

$$I_v = \{f \in Rz \oplus R \mid f(P_i, v_i) = 0, 1 \leq i \leq n\}.$$

Then it is easy to see that  $I_v = R(z - h_v) + J$  where

$$h_v = \sum_{i=1}^n v_i h_i, \quad J = \bigcap_{i=1}^n \mathfrak{m}_i.$$

As  $J$  is an ideal of  $R$ ,  $J$  is a free  $\mathbb{F}[x]$ -submodule of  $R$  of rank  $a$  and has a Gröbner basis  $\{\eta_0, \eta_1, \dots, \eta_{a-1}\}$  with respect to  $>_\delta$  such that  $\deg_y(\text{lt}(\eta_i)) = i$ . Then

$$\sum_{0 \leq i < a} \deg_x(\text{lt}(\eta_i)) = \dim_{\mathbb{F}} R/J = n. \quad (1)$$

As  $I_v = R(z - h_v) + J$ , the set

$$\{\eta_0, \eta_1, \dots, \eta_{a-1}, z - h_v, y(z - h_v), \dots, y^{a-1}(z - h_v)\} \quad (2)$$

is a Gröbner basis of  $I_v$  with respect to  $>_{\delta(h_v)}$ .

The ideal of the error vector  $e$

$$J_e = \bigcap_{e_i \neq 0} \mathfrak{m}_i$$

also has a Gröbner basis  $\{\epsilon_0, \epsilon_1, \dots, \epsilon_{a-1}\}$  with respect to  $>_\delta$  such that  $\deg_y(\text{lt}(\epsilon_i)) = i$ . Then

$$\sum_{0 \leq i < a} \deg_x(\text{lt}(\epsilon_i)) = \dim_{\mathbb{F}} R/J_e = \text{wt}(e). \quad (3)$$

The results in the following Section III-A will serve as a backbone of our decoding algorithm presented in Section III-B and its proof in Section III-C.

#### A. Decoding by Majority Voting

Let  $s$  be a nongap with  $s \leq u$ . Suppose

$$v^{(s)} = e + \text{ev}(\mu^{(s)}), \quad \mu^{(s)} = \omega_s \varphi_s + \mu^{(s-1)}, \quad \mu^{(s-1)} \in L_{s-1},$$

and  $B^{(s)} = \{g_i^{(s)}, f_i^{(s)} \mid 0 \leq i < a\}$  is a Gröbner basis of  $I_{v^{(s)}}$  with respect to  $>_s$  where

$$\begin{aligned} g_i^{(s)} &= \sum_{0 \leq j < a} c_{i,j} y^j z + \sum_{0 \leq j < a} d_{i,j} y^j, \quad c_{i,j}, d_{i,j} \in \mathbb{F}[x], \\ f_i^{(s)} &= \sum_{0 \leq j < a} a_{i,j} y^j z + \sum_{0 \leq j < a} b_{i,j} y^j, \quad a_{i,j}, b_{i,j} \in \mathbb{F}[x] \end{aligned}$$

such that  $\text{lt}(g_i^{(s)}) = \text{lt}(d_{i,i} y^i)$  and  $\text{lt}(f_i^{(s)}) = \text{lt}(a_{i,i} y^i z)$  for  $0 \leq i < a$ . Let  $\nu_i^{(s)} = \text{lc}(d_{i,i})$ .

**Lemma 2.** *We have*

$$\sum_{0 \leq i < a} \deg(a_{i,i}) + \sum_{0 \leq i < a} \deg(d_{i,i}) = n.$$

*Proof:* As  $B^{(s)}$  is a Gröbner basis of  $I_{v^{(s)}}$ ,

$$\sum_{0 \leq i < a} \deg(a_{i,i}) + \sum_{0 \leq i < a} \deg(d_{i,i}) = \dim_{\mathbb{F}} (Rz \oplus R) / I_{v^{(s)}}.$$

Since  $I_{v^{(s)}} = R(z - h_{v^{(s)}}) + J$ , we have  $\dim_{\mathbb{F}}(Rz \oplus R)/I_{v^{(s)}} = \dim_{\mathbb{F}} R/J = n$ .  $\square$

**Lemma 3.** For  $0 \leq i < a$ , we have  $\delta(a_{i,i}y^i) \leq \delta(\epsilon_i)$ , equivalently  $\deg(a_{i,i}) \leq \deg_x(\text{lt}(\epsilon_i))$ .

*Proof:* Since  $J_e(z - \mu^{(s)}) \subset I_{v^{(s)}}$ , we have  $\epsilon_i(z - \mu^{(s)}) \in I_{v^{(s)}}$ . Note that  $\text{lt}(\epsilon_i(z - \mu^{(s)})) = \text{lt}(\epsilon_i z)$  with respect to  $>_s$ , and  $\deg_y(\epsilon_i z) = i$ . As  $B^{(s)}$  is a Gröbner basis of  $I_{v^{(s)}}$ , the leading term  $\text{lt}(\epsilon_i z)$  must be an  $\mathbb{F}[x]$ -multiple of  $\text{lt}(f_i^{(s)})$ . Thus the assertion follows.  $\square$

**Lemma 4.** For  $0 \leq i < a$ , we have  $\delta(d_{i,i}y^i) \leq \delta(\eta_i)$ , equivalently  $\deg(d_{i,i}) \leq \deg_x(\text{lt}(\eta_i))$ .

*Proof:* As  $B^{(s)}$  is a Gröbner basis of  $I_{v^{(s)}}$  and  $J \subset I_{v^{(s)}}$ , it follows that  $\eta_i$  is an  $\mathbb{F}[x]$ -multiple of  $\text{lt}(g_i^{(s)})$ . Hence the assertion follows.  $\square$

Now let  $w$  be any element of  $\mathbb{F}$ . For each  $0 \leq i < a$ , let

$$\bar{g}_i = g_i^{(s)}(z + w\varphi_s), \quad \bar{f}_i = f_i^{(s)}(z + w\varphi_s)$$

where the parentheses denote substitution of the variable  $z$ . The automorphism of the ring  $R[z]$  induced by the substitution  $z \mapsto z + w\varphi_s$  preserves leading terms with respect to  $>_s$ . Therefore the set  $\bar{B} = \{\bar{g}_i, \bar{f}_i \mid 0 \leq i < a\}$  is a Gröbner basis of

$$\tilde{I} = \{f(z + w\varphi_s) \mid f \in I_{v^{(s)}}\}$$

with respect to  $>_s$ . However, with respect to  $>_{s-1}$ ,  $\bar{B}$  is generally no longer a Gröbner basis of  $\tilde{I}$ . The following procedure modifies  $\bar{B}$  to obtain a Gröbner basis of  $\tilde{I}$  with respect to  $>_{s-1}$ .

For each  $0 \leq i < a$ , there are unique integers  $0 \leq i' < a = \delta_x$  and  $k_i$  satisfying

$$\delta(a_{i,i}y^i) + s = \delta_x k_i + \delta_y i'. \quad (4)$$

Then let

$$c_i = \deg_x(d_{i',i'}) - k_i, \quad \bar{c}_i = \max\{c_i, 0\} \quad (5)$$

and

$$w_i = -\frac{b_{i,i'}[x^{k_i}]}{\mu_i}, \quad \mu_i = \text{lc}(a_{i,i}y^i\varphi_s). \quad (6)$$

Note that the map  $i \mapsto i'$  is a permutation of  $\{0, 1, \dots, a-1\}$  and that the integer  $c_i$  is defined such that

$$\delta_x c_i = \delta(d_{i',i'}y^{i'}) - \delta(a_{i,i}y^i) - s. \quad (7)$$

Now if  $w_i = w$ , let

$$\tilde{g}_{i'} = \bar{g}_{i'}, \quad \tilde{f}_i = \bar{f}_i \quad (8)$$

and if  $w_i \neq w$  and  $c_i > 0$ , let

$$\tilde{g}_{i'} = \bar{f}_i, \quad \tilde{f}_i = x^{c_i} \bar{f}_i - \frac{\mu_i(w - w_i)}{\nu_{i'}^{(s)}} \bar{g}_{i'} \quad (9)$$

and if  $w_i \neq w$  and  $c_i \leq 0$ , let

$$\tilde{g}_{i'} = \bar{g}_{i'}, \quad \tilde{f}_i = \bar{f}_i - \frac{\mu_i(w - w_i)}{\nu_{i'}^{(s)}} x^{-c_i} \bar{g}_{i'}. \quad (10)$$

**Proposition 5.** The set  $\tilde{B} = \{\tilde{g}_i, \tilde{f}_i \mid 0 \leq i < a\}$  is a Gröbner basis of  $\tilde{I}$  with respect to  $>_{s-1}$ .

*Proof:* Let  $0 \leq i < a$ . We consider the pair

$$\begin{aligned} \bar{g}_{i'} &= \sum_{0 \leq j < a} c_{i',j} y^j z + \sum_{0 \leq j < a} d_{i',j} y^j + \sum_{0 \leq j < a} w c_{i',j} y^j \varphi_s, \\ \bar{f}_i &= \sum_{0 \leq j < a} a_{i,j} y^j z + \sum_{0 \leq j < a} b_{i,j} y^j + \sum_{0 \leq j < a} w a_{i,j} y^j \varphi_s. \end{aligned}$$

By the assumption that  $B^{(s)}$  is a Gröbner basis of  $I_{v^{(s)}}$  with respect to  $>_s$ , we have for  $0 \leq j < a$ ,

$$\delta(d_{i',i'}y^{i'}) > \delta_s(c_{i',j}y^j z) \geq \delta(w c_{i',j}y^j \varphi_s)$$

and for  $0 \leq j < a$  with  $j \neq i'$ ,  $\delta(d_{i',j}y^j) > \delta(d_{i',i'}y^{i'})$ . Therefore with respect to  $>_{s-1}$ ,  $\text{lt}(\bar{g}_{i'}) = \text{lt}(d_{i',i'}y^{i'})$ . By the same assumption, we have for  $0 \leq j < a$  with  $j \neq i$ ,

$$\delta_s(a_{i,i}y^i z) > \delta_s(a_{i,j}y^j z) \geq \delta(wa_{i,j}y^j \varphi_s)$$

and for  $0 \leq j < a$  with  $j \neq i'$ ,  $\delta_s(a_{i,i}y^i z) > \delta(b_{i,j}y^j)$  by the definition of  $i'$  in (4). Note that

$$\delta_s(a_{i,i}y^i z) \geq \delta(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s) \quad (11)$$

where the inequality is strict if and only if  $w = w_i$  by the definition of  $w_i$  in (6).

From now on, all leading terms are with respect to  $>_{s-1}$ . The inequality (11) implies that if  $w = w_i$ , then  $\text{lt}(\bar{f}_i) = \text{lt}(a_{i,i}y^i z)$  and if  $w \neq w_i$ , then  $\text{lt}(\bar{f}_i) = \text{lt}(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s)$ .

First we consider the case that  $w_i = w$ . By (8),

$$\text{lt}(\tilde{g}_{i'}) = \text{lt}(\bar{g}_{i'}) = \text{lt}(d_{i',i'}y^{i'}), \quad \text{lt}(\tilde{f}_i) = \text{lt}(\bar{f}_i) = \text{lt}(a_{i,i}y^i z). \quad (12)$$

Next we consider the case that  $w_i \neq w$  and  $c_i > 0$ . Then we have (9). Note that

$$\text{lt}(x^{c_i} \bar{f}_i) = x^{c_i} \text{lt}(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s), \quad \text{lt}(\bar{g}_{i'}) = \text{lt}(d_{i',i'}y^{i'})$$

and

$$\delta_x c_i + \delta(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s) = \delta_x c_i + \delta_s(a_{i,i}y^i z) = \delta(d_{i',i'}y^{i'})$$

where the second equality is from (7), and

$$\text{lc}(x^{c_i} \bar{f}_i) = \text{lc}(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s) = -\mu_i w_i + \mu_i w = \text{lc}\left(\frac{\mu_i(w - w_i)}{\nu_{i'}^{(s)}} \bar{g}_{i'}\right).$$

Therefore, together with (11),

$$\text{lt}(\tilde{f}_i) = \text{lt}(x^{c_i} a_{i,i}y^i z), \quad \text{lt}(\tilde{g}_{i'}) = \text{lt}(\bar{f}_i) = \text{lt}(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s). \quad (13)$$

For the case that  $w_i \neq w$  and  $c_i \leq 0$ , we have (10). By repeating almost the same argument as above, we can show that

$$\text{lt}(\tilde{g}_{i'}) = \text{lt}(d_{i',i'}y^{i'}), \quad \text{lt}(\tilde{f}_i) = \text{lt}(a_{i,i}y^i z). \quad (14)$$

Finally it is clear that  $\tilde{B}$  generates the module  $\tilde{I}$ . From (12), (13), and (14), we see that  $\tilde{B}$  is a Gröbner basis of  $\tilde{I}$  with respect to  $>_{s-1}$ , by the criterion in Proposition 1.  $\square$

**Lemma 6.** *Let  $0 \leq i < a$ . If  $w_i \neq w$ , then*

$$\delta_{s-1}(\tilde{g}_{i'}) = \delta(d_{i',i'}y^{i'}) - \delta_x \bar{c}_i, \quad \delta_{s-1}(\tilde{f}_i) = \delta_{s-1}(a_{i,i}y^i z) + \delta_x \bar{c}_i. \quad (15)$$

*Proof:* Suppose  $w_i \neq w$ . Let us show the first equation. If  $c_i > 0$ , then

$$\delta_{s-1}(\tilde{g}_{i'}) = \delta_{s-1}(\bar{f}_i) = \delta(b_{i,i'}y^{i'} + wa_{i,i}y^i \varphi_s) = \delta_s(a_{i,i}y^i z) = \delta(d_{i',i'}y^{i'}) - \delta_x c_i,$$

by (13), (11), and (7). If  $c_i \leq 0$ , then  $\delta_{s-1}(\tilde{g}_{i'}) = \delta(d_{i',i'}y^{i'})$  by (14). The second equation is clear by (13) and (14).  $\square$

**Proposition 7.** *For  $i$  with  $w_i \neq \omega_s$ ,*

$$\delta(\epsilon_i) - \delta(a_{i,i}y^i) \geq \delta_x \bar{c}_i \quad \text{and} \quad \min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} \geq \delta(d_{i',i'}y^{i'}).$$

*Proof:* Suppose  $w_i \neq \omega_s$ . Then let us set  $w = \omega_s$ . Since  $J_e(z - \omega_s \varphi_s - \mu^{(s-1)}) \subset I_{v^{(s)}}$ , we have

$$J_e(z - \mu^{(s-1)}) \subset \tilde{I}.$$

In particular,  $\epsilon_i(z - \mu^{(s-1)}) \in \tilde{I}$ . Note that with respect to  $>_{s-1}$ ,  $\text{lt}(\epsilon_i(z - \mu^{(s-1)})) = \text{lt}(\epsilon_i z)$ . As  $\tilde{B}$  is a Gröbner basis of  $\tilde{I}$  with respect to  $>_{s-1}$ ,  $\text{lt}(\epsilon_i z)$  must be an  $\mathbb{F}[x]$ -multiple of the leading term of  $\tilde{f}_i$ . With (15), this implies  $\delta(a_{i,i}y^i) + \delta_x \bar{c}_i \leq \delta(\epsilon_i)$ . Now by (7),

$$\delta(\epsilon_i) - \delta(a_{i,i}y^i) \geq \delta_x \bar{c}_i \geq \delta_x c_i = \delta(d_{i',i'}y^{i'}) - \delta(a_{i,i}y^i) - s.$$

Hence  $\delta(\epsilon_i) + s \geq \delta(d_{i',i'}y^{i'})$ . □

**Proposition 8.** For  $i$  with  $w_i = \omega_s$ ,

$$\min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} \geq \delta(d_{i',i'}y^{i'}) - \delta_x \bar{c}_i$$

*Proof:* Suppose  $w_i = \omega_s$ . Then let us choose  $w \in \mathbb{F}$  such that  $w \neq w_i$ . Since  $J_e(z - \omega_s \varphi_s - \mu^{(s-1)}) \subset I_{v(s)}$ , we have

$$J_e(z - (\omega_s - w)\varphi_s - \mu^{(s-1)}) \subset \tilde{I}.$$

In particular,  $\epsilon_i(z - (\omega_s - w)\varphi_s - \mu^{(s-1)}) \in \tilde{I}$ . Note that  $\omega_s - w \neq 0$ . With respect to  $>_{s-1}$ ,

$$\text{lt}(\epsilon_i(z - (\omega_s - w)\varphi_s - \mu^{(s-1)})) = \text{lt}((\omega_s - w)\epsilon_i\varphi_s)$$

As  $\tilde{B}$  is a Gröbner basis of  $\tilde{I}$  with respect to  $>_{s-1}$ ,  $\text{lt}((\omega_s - w)\epsilon_i\varphi_s)$  must be a scalar multiple of the leading term of  $\tilde{g}_{i'}$ . With (15), this implies  $\delta(\epsilon_i) + s \geq \delta(d_{i',i'}y^{i'}) - \delta_x \bar{c}_i$ . Finally,  $\delta(\eta_{i'}) \geq \delta(d_{i',i'}y^{i'}) \geq \delta(d_{i',i'}y^{i'}) - \delta_x \bar{c}_i$ . □

**Proposition 9.** The condition

$$\sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, \delta(\epsilon_i) - \delta(y^i)\} > 2\delta_x \text{wt}(e)$$

implies

$$\sum_{w_i = \omega_s} \bar{c}_i > \sum_{w_i \neq \omega_s} \bar{c}_i.$$

*Proof:* Propositions 7 and 8 imply

$$\begin{aligned} \sum_{w_i = \omega_s} \delta_x \bar{c}_i &\geq \sum_{w_i = \omega_s} \delta(d_{i',i'}y^{i'}) - \min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} \\ &\geq \sum_{0 \leq i < a} \delta(d_{i',i'}y^{i'}) - \min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} \end{aligned}$$

and

$$\sum_{w_i \neq \omega_s} \delta_x \bar{c}_i \leq \sum_{w_i \neq \omega_s} \delta(\epsilon_i) - \delta(a_{i,i}y^i) \leq \sum_{0 \leq i < a} \delta(\epsilon_i) - \delta(a_{i,i}y^i).$$

Now we have a chain of equivalent conditions

$$\begin{aligned} \sum_{0 \leq i < a} \delta(d_{i',i'}y^{i'}) - \min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} &> \sum_{0 \leq i < a} \delta(\epsilon_i) - \delta(a_{i,i}y^i) \\ \iff \sum_{0 \leq i < a} \delta(d_{i',i'}y^{i'}) + \sum_{0 \leq i < a} \delta(a_{i,i}y^i) - \min\{\delta(\epsilon_i) + s, \delta(\eta_{i'})\} &> \sum_{0 \leq i < a} \delta(\epsilon_i) \\ \iff \sum_{0 \leq i < a} \delta(\eta_{i'}) + \sum_{0 \leq i < a} \delta(y^i) + \max\{-\delta(\epsilon_i) - s, -\delta(\eta_{i'})\} &> \sum_{0 \leq i < a} \delta(\epsilon_i) \\ \iff \sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, \delta(\epsilon_i) - \delta(y^i)\} &> \sum_{0 \leq i < a} 2(\delta(\epsilon_i) - \delta(y^i)) \end{aligned}$$

where we used the equality

$$\begin{aligned} \sum_{0 \leq i < a} \delta(d_{i',i'}y^{i'}) + \sum_{0 \leq i < a} \delta(a_{i,i}y^i) &= \sum_{0 \leq i < a} \delta(d_{i,i}y^i) + \sum_{0 \leq i < a} \delta(a_{i,i}y^i) \\ &= \sum_{0 \leq i < a} (\delta(d_{i,i}) + \delta(a_{i,i})) + \sum_{0 \leq i < a} 2\delta(y^i) \\ &= \delta_x n + \sum_{0 \leq i < a} 2\delta(y^i) \\ &= \sum_{0 \leq i < a} (\delta(\eta_i) - \delta(y^i)) + \sum_{0 \leq i < a} 2\delta(y^i) \\ &= \sum_{0 \leq i < a} \delta(\eta_{i'}) + \sum_{0 \leq i < a} \delta(y^i) \end{aligned}$$

shown by Lemma 2 and (1). Finally note that

$$\sum_{0 \leq i < a} 2(\delta(\epsilon_i) - \delta(y^i)) = \sum_{0 \leq i < a} 2\delta_x \deg_x(\epsilon_i) = 2\delta_x \text{wt}(e)$$

by (3). □

**Proposition 10.** *Let*

$$\nu(s) = \frac{1}{\delta_x} \sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, 0\}.$$

*The condition  $\nu(s) > 2\text{wt}(e)$  implies*

$$\sum_{w_i = \omega_s} \bar{c}_i > \sum_{w_i \neq \omega_s} \bar{c}_i.$$

*Proof:* We have

$$\sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, \delta(\epsilon_i) - \delta(y^i)\} \geq \sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, 0\}$$

as  $\delta(\epsilon_i) - \delta(y^i) \geq 0$  for  $0 \leq i < a$ . □

### B. Decoding Algorithm

*a) Initialization:* Let  $N = \delta(h_v)$ , and let  $B^{(N)}$  be the Gröbner basis of  $I_v$  with respect to  $>_N$  given in (2). The steps *Pairing*, *Voting*, *Rebasing* are iterated for  $s$  decreasing from  $N$  to 0.

*b) Pairing:* Suppose  $B^{(s)} = \{g_i^{(s)}, f_i^{(s)} \mid 0 \leq i < a\}$  is a Gröbner basis of  $I_{v^{(s)}}$  with respect to  $>_s$  where

$$\begin{aligned} g_i^{(s)} &= \sum_{0 \leq j < a} c_{i,j} y^j z + \sum_{0 \leq j < a} d_{i,j} y^j \\ f_i^{(s)} &= \sum_{0 \leq j < a} a_{i,j} y^j z + \sum_{0 \leq j < a} b_{i,j} y^j \end{aligned}$$

and let  $\nu_i^{(s)} = \text{lc}(d_{i,i})$ . For  $0 \leq i < a$ , there are unique integers  $0 \leq i' < \delta_x = a$  and  $k_i$  satisfying

$$\delta(a_{i,i} y^{i'}) + s = \delta_x k_i + \delta_y i'.$$

Note that the integer  $\delta(a_{i,i} y^{i'}) + s$  is a nongap if and only if  $k_i \geq 0$ . Now let

$$c_i = \deg_x(d_{i',i'}) - k_i.$$

*c) Voting:* If  $s > u$  or  $s$  is a gap, then for  $i$  with nongap  $\delta(a_{i,i} y^{i'}) + s$ , let

$$w_i = -b_{i,i'}[x^{k_i}], \quad \mu_i = 1$$

and for  $i$  with gap  $\delta(a_{i,i} y^{i'}) + s$ , let  $w_i = 0, \mu_i = 1$ . Let  $w = 0$  in both cases.

If  $s \leq u$  and  $s$  is a nongap, then for each  $i$ , we let

$$w_i = -\frac{b_{i,i'}[x^{k_i}]}{\mu_i}, \quad \mu_i = \text{lc}(a_{i,i} y^{i'} \varphi_s)$$

and let  $\bar{c}_i = \max\{c_i, 0\}$ , and let  $w$  be the element of  $\mathbb{F}$  with the largest

$$\sum_{w=w_i} \bar{c}_i,$$

and let  $w_s = w$ .



d) *Rebasing*: For each  $i$ , we do the following. If  $w_i = w$ , then let

$$\begin{aligned} g_{i'}^{(s-1)} &= g_{i'}^{(s)}(z + w\varphi_s) \\ f_i^{(s-1)} &= f_i^{(s)}(z + w\varphi_s) \end{aligned} \quad (16)$$

and let  $\nu_{i'}^{(s-1)} = \nu_{i'}^{(s)}$ . If  $w_i \neq w$  and  $c_i > 0$ , then let

$$\begin{aligned} g_{i'}^{(s-1)} &= f_i^{(s)}(z + w\varphi_s) \\ f_i^{(s-1)} &= x^{c_i} f_i^{(s)}(z + w\varphi_s) - \frac{\mu_i(w - w_i)}{\nu_{i'}^{(s)}} g_{i'}^{(s)}(z + w\varphi_s) \end{aligned} \quad (17)$$

and let  $\nu_{i'}^{(s-1)} = \mu_i(w - w_i)$ . If  $w_i \neq w$  and  $c_i \leq 0$ , then let

$$\begin{aligned} g_{i'}^{(s-1)} &= g_{i'}^{(s)}(z + w\varphi_s) \\ f_i^{(s-1)} &= f_i^{(s)}(z + w\varphi_s) - \frac{\mu_i(w - w_i)}{\nu_{i'}^{(s)}} x^{-c_i} g_{i'}^{(s)}(z + w\varphi_s) \end{aligned} \quad (18)$$

and let  $\nu_{i'}^{(s-1)} = \nu_{i'}^{(s)}$ . Let  $B^{(s-1)} = \{g_i^{(s-1)}, f_i^{(s-1)} \mid 0 \leq i < a\}$ .

e) *Termination*: After the iterations, output the recovered message  $(w_{s_1}, w_{s_2}, \dots, w_{s_k})$ .

### C. Proof of the Algorithm

Let us start with a brief overview of the algorithm. Note that the decoding algorithm is in one of two phases while  $s$  decreases from  $N$  to 0. The first phase is when  $s > u$  or  $s$  is a gap, and the second phase is when  $s \leq u$  and  $s$  is a nongap. Let  $v^{(N)} = v$ . In the first phase, the Gröbner basis  $B^{(s)}$  of  $I_{v^{(s)}}$  with respect to  $>_s$  is updated such that  $B^{(s-1)}$  is a Gröbner basis of  $I_{v^{(s-1)}}$  with respect to  $>_{s-1}$  where

$$v^{(s-1)} = v^{(s)}.$$

In the second phase, the algorithm determines  $w_s$  by majority voting and updates  $B^{(s)}$  such that  $B^{(s-1)}$  is a Gröbner basis of  $I_{v^{(s-1)}}$  with respect to  $>_{s-1}$  where

$$v^{(s-1)} = v^{(s)} - \text{ev}(w_s \varphi_s).$$

When the algorithm terminates,  $w_s$  are determined for all nongaps  $s \leq u$ .

**Proposition 11.** For  $N \geq s \geq 0$ , the set  $B^{(s)}$  is a Gröbner basis of  $I_{v^{(s)}}$  with respect to  $>_s$ .

*Proof:* This is proved by induction on  $s$ . For  $s = N$ , this is true by (2). Now our induction assumption is that this is true for  $s$ . In the second phase, we already saw in Proposition 5 that  $B^{(s-1)}$  is a Gröbner basis of  $I_{v^{(s-1)}}$ . So it remains to consider the first phase. The proof for this case is similar to that of Proposition 5.

Suppose  $s > u$  or  $s$  is a gap. Let  $0 \leq i < a$ . Recall

$$\begin{aligned} g_{i'}^{(s)} &= \sum_{0 \leq j < a} c_{i',j} y^j z + \sum_{0 \leq j < a} d_{i',j} y^j \\ f_i^{(s)} &= \sum_{0 \leq j < a} a_{i,j} y^j z + \sum_{0 \leq j < a} b_{i,j} y^j \end{aligned}$$

By the induction assumption, we have for  $0 \leq j < a$ ,

$$\delta(d_{i',i'} y^{i'}) > \delta_s(c_{i',j} y^j z) = \delta(c_{i',j} y^j) + s$$

and for  $0 \leq j < a$  with  $j \neq i'$ ,  $\delta(d_{i',i'} y^{i'}) > \delta(d_{i',j} y^j)$ . Therefore with respect to  $>_{s-1}$ ,  $\text{lt}(g_{i'}^{(s)}) = \text{lt}(d_{i',i'} y^{i'})$ . Similarly, by the induction assumption, we have for  $0 \leq j < a$  with  $j \neq i$ ,  $\delta_s(a_{i,i} y^i z) > \delta_s(a_{i,j} y^j z)$  and for  $0 \leq j < a$  with  $j \neq i'$ ,  $\delta_s(a_{i,i} y^i z) > \delta(b_{i,j} y^j)$ .

Note that

$$\delta_s(a_{i,i} y^i z) \geq \delta(b_{i,i'} y^{i'}) \quad (19)$$

where the inequality is strict except when  $\delta(a_{i,i}y^i) + s$  is a nongap and  $b_{i,i'}[x^{k_i}] \neq 0$ . Note that  $w_i = 0$  if and only if  $\delta(a_{i,i}y^i) + s$  is a gap or  $\delta(a_{i,i}y^i) + s$  is a nongap but  $b_{i,i'}[x^{k_i}] = 0$ . Therefore with respect to  $>_{s-1}$  if  $w_i = 0$ , then  $\text{lt}(f_i^{(s)}) = \text{lt}(a_{i,i}y^i z)$  and if  $w_i \neq 0$ , then  $\text{lt}(f_i^{(s)}) = \text{lt}(b_{i,i'}y^{i'})$ .

Now let us consider the case when  $w_i = 0$ , then by (16) and (19),

$$\text{lt}(g_{i'}^{(s-1)}) = \text{lt}(g_{i'}^{(s)}) = \text{lt}(d_{i',i'}y^{i'}), \quad \text{lt}(f_i^{(s-1)}) = \text{lt}(f_i^{(s)}) = \text{lt}(a_{i,i}y^i z).$$

with respect to  $>_{s-1}$ . We consider the case when  $w_i \neq 0$  and  $c_i > 0$ . Then by (17),

$$g_{i'}^{(s-1)} = f_i^{(s)}, \quad f_i^{(s-1)} = x^{c_i} f_i^{(s)} + \frac{\mu_i w_i}{\nu_{i'}^{(s)}} g_{i'}^{(s)}.$$

Note that

$$\begin{aligned} \text{lt}(x^{c_i} f_i^{(s)}) &= x^{c_i} \text{lt}(b_{i,i'}y^{i'}), \quad \text{lt}(g_{i'}^{(s)}) = \text{lt}(d_{i',i'}y^{i'}), \\ c_i \delta_x + \delta(b_{i,i'}y^{i'}) &= c_i \delta_x + \delta(a_{i,i}y^i z) = \delta(d_{i',i'}y^{i'}), \end{aligned}$$

and

$$\text{lc}(x^{c_i} f_i^{(s)}) = \text{lc}(b_{i,i'}y^{i'}) = -\mu_i w_i = -\text{lc}\left(\frac{\mu_i w_i}{\nu_{i'}^{(s)}} g_{i'}^{(s)}\right).$$

Together with (19), this implies  $\text{lt}(f_i^{(s-1)}) = \text{lt}(x^{c_i} a_{i,i}y^i z)$ .

For the case when  $w_i \neq 0$  and  $c_i \leq 0$ , we have by (18)

$$g_{i'}^{(s-1)} = g_{i'}^{(s)}, \quad f_i^{(s-1)} = f_i^{(s)} + \frac{\mu_i w_i}{\nu_{i'}^{(s)}} x^{-c_i} g_{i'}^{(s)}.$$

By the same argument as when  $c_i > 0$ , we can show that  $\text{lt}(f_i^{(s-1)}) = \text{lt}(a_{i,i}y^i z)$ .

Hence the set  $B^{(s-1)}$  is again a Gröbner basis of  $I_{v^{(s-1)}}$  with respect to  $>_{s-1}$ . □

**Proposition 12.** *Let*

$$d_u = \min\{\nu(s) \mid s \in S, s \leq u\}.$$

*Then  $d_u \geq n - u$ . If  $2\text{wt}(e) < d_u$ , then  $w_s = \omega_s$  for all  $s \in S, s \leq u$ . Hence*

$$\sum_{s \in S, s \leq u} w_s \varphi_s = \mu.$$

*Proof:* The bound  $d_u \geq n - u$  follows from

$$\begin{aligned} \nu(s) &= \frac{1}{\delta_x} \sum_{0 \leq i < a} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, 0\} \\ &\geq \frac{1}{\delta_x} \sum_{0 \leq i < a} (\delta(\eta_{i'}) - \delta(y^i) - s) \\ &= \frac{1}{\delta_x} \sum_{0 \leq i < a} (\delta(\eta_i) - \delta(y^i)) - s = n - s. \end{aligned}$$

If we suppose  $2\text{wt}(e) < d_u$ , then Propositions 10 and 11 imply  $w_s = \omega_s$  for all  $s \in S, s \leq u$ . □

#### IV. HERMITIAN CODES

A Hermitian curve  $H$  is a smooth plane curve defined with the equation  $y^q + y = x^{q+1}$  over  $\mathbb{F}_{q^2}$ . It has  $q^3$  rational points  $P_i$  with a unique nonsingular point  $P_\infty$  at infinity. The functions  $x$  and  $y$  on  $H$  have poles at  $P_\infty$  of orders  $q$  and  $q + 1$ , respectively. That is,  $\delta_x = q$ ,  $\delta_y = q + 1$ .

The ideal  $J$  associated with the sum of  $P_i$  is an  $\mathbb{F}[x]$ -module generated by

$$\eta_i = y^i(x^{q^2} - x), \quad 0 \leq i < q$$

which form a Gröbner basis of  $J$  with respect to  $>_\delta$ .

**Proposition 13.** For nongap  $s < q^3$ ,

$$\nu(s) = (q-r)(q^2+r-t) + r \max\{q^2+r-q-t-1, 0\}$$

where  $s = tq + r$ ,  $0 \leq r < q$ .

*Proof:* Suppose

$$\delta(y^i) + s = (q+1)i + s = aq + i'(q+1), \quad 0 \leq i' < q.$$

Then  $\delta(\eta_{i'}) = q^3 + i'(q+1)$ . As  $i' = (s+i) \bmod q$ ,

$$\begin{aligned} \nu(s) &= \frac{1}{q} \sum_{i=0}^{q-1} \max\{\delta(\eta_{i'}) - \delta(y^i) - s, 0\} \\ &= \frac{1}{q} \sum_{i=0}^{q-1} \max\{q^3 + ((s+i) \bmod q)(q+1) - (q+1)i - s, 0\} \\ &= \frac{1}{q} \sum_{i=0}^{q-1} \max\{q^3 - qi + ((s+i) \bmod q)q - ((s+i) - (s+i) \bmod q), 0\} \\ &= \sum_{i=0}^{q-1} \max\{q^2 - i + (s+i) \bmod q - \lfloor (s+i)/q \rfloor, 0\}. \end{aligned}$$

Now let  $s = tq + r$ ,  $0 \leq t < q^2$ ,  $0 \leq r < q$ . Then

$$\begin{aligned} \nu(s) &= \sum_{i=0}^{q-1} \max\{q^2 - i + (r+i) \bmod q - t - \lfloor (r+i)/q \rfloor, 0\} \\ &= \sum_{i=0}^{q-1-r} \max\{q^2 - i + r + i - t, 0\} + \sum_{i=q-r}^{q-1} \max\{q^2 - i + r + i - q - t - 1, 0\} \\ &= (q-r)(q^2+r-t) + r \max\{q^2+r-q-t-1, 0\}. \end{aligned}$$

□

**Proposition 14.** For nongap  $u < q^3$ ,

$$d_u = \min\{\nu(s) \mid \text{nongap } s \leq u\} = \begin{cases} q^3 - aq & \text{if } b \leq a - (q^2 - q), \\ q^3 - u & \text{if } b > a - (q^2 - q), \end{cases}$$

where  $u = aq + b$ ,  $0 \leq b < q$ .

*Proof:* For nongap  $s = tq + r$ ,

$$\begin{aligned} \nu(s) &= (q-r)(q^2+r-t) + r \max\{q^2+r-q-t-1, 0\} \\ &= q^3 - tq + r \max\{-1, t - q^2 + q - r\} \geq q^3 - s. \end{aligned}$$

So we see that if  $a - q^2 + q - b \geq 0$ , that is,  $b \leq a - (q^2 - q)$ , then the minimum

$$\nu(aq) = q^3 - aq$$

is attained when  $s = aq$ , and hence  $d_u = q^3 - aq$ . On the other hand, if  $b > a - (q^2 - q)$ , then

$$\nu(u) = q^3 - aq - b = q^3 - u$$

is the minimum, and therefore  $d_u = q^3 - u$ . □

It can be shown that the bound  $d_u$  exactly matches with the order bound on the minimum distance of Hermitian codes as given in [12] and [13]. Hence we may call  $d_u$  also an order bound. Figures 1 and 2 show the order bounds for Hermitian codes with  $q = 3$  and  $q = 8$ , respectively.

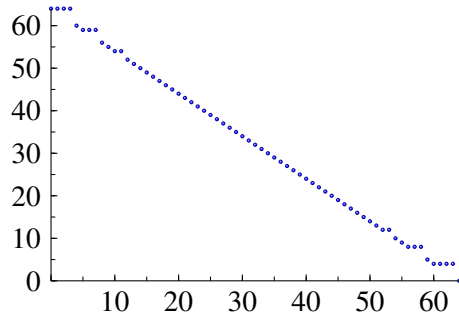


Fig. 1. Order bound for Hermitian code over  $\mathbb{F}_{16}$

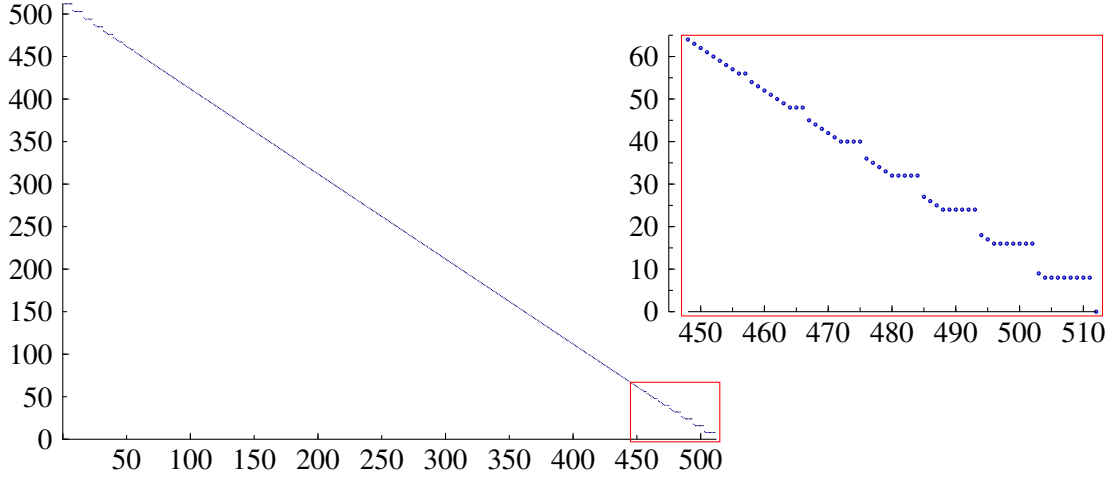


Fig. 2. Order bound for Hermitian codes over  $\mathbb{F}_{64}$

Let  $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$  with  $\alpha^2 - \alpha - 1 = 0$ . We use the Hermitian curve over  $\mathbb{F}_9$  defined by  $y^3 + y = x^4$ , which has 27 rational points

$$(0, 0), (0, \alpha^2), (0, \alpha^6), (1, 2), (1, \alpha), (1, \alpha^3), (2, 2), (2, \alpha), (2, \alpha^3), (\alpha, 1), (\alpha, \alpha^7), (\alpha, \alpha^5), (\alpha^2, 2), (\alpha^2, \alpha), (\alpha^2, \alpha^3), (\alpha^7, 1), (\alpha^7, \alpha^7), (\alpha^7, \alpha^5), (\alpha^5, 1), (\alpha^5, \alpha^7), (\alpha^5, \alpha^5), (\alpha^3, 1), (\alpha^3, \alpha^7), (\alpha^3, \alpha^5), (\alpha^6, 2), (\alpha^6, \alpha), (\alpha^6, \alpha^3)$$

to define the Hermitian code  $C_{16}$ , [27, 14, 11] linear code over  $\mathbb{F}_9$ .

Suppose that the sent codeword was corrupted during the transmission, and the received vector is

$$v = (0, 0, 0, 0, 0, \alpha^2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^3, 0, 0, \alpha^7, 0, 0, 2, 0).$$

The six generators of the module  $I_v$  are

$$\begin{aligned} g_0 &= x^9 - x, \\ g_1 &= y(x^9 - x), \\ g_2 &= y^2(x^9 - x), \\ f_0 &= z - h_v, \\ f_1 &= y(z - h_v), \\ f_2 &= y^2(z - h_v), \end{aligned}$$

where

$$\begin{aligned} h_v &= (\alpha^3 x^8 + x^7 + \alpha^7 x^6 + \alpha^5 x^5 + \alpha^3 x^4 + \alpha^6 x^3 + 2x^2 + \alpha^2 x)y^2 \\ &\quad + (\alpha^6 x^8 + x^7 + x^6 + \alpha x^5 + \alpha^6 x^4 + \alpha^7 x^3 + \alpha^3 x)y \\ &\quad + 2x^8 + \alpha x^7 + \alpha^6 x^6 + 2x^4 + \alpha^2 x^3 + x. \end{aligned}$$

Note that  $N = \delta(h_v) = 32$ . Thus the initial basis for the code  $C_{16}$  is

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$						$x^9 + \dots$
$g_1$					$x^9 + \dots$	
$g_2$				$x^9 + \dots$		
$f_0$			1	$\alpha^7x^8 + \dots$	$\alpha^2x^8 + \dots$	$x^8 + \dots$
$f_1$		1		$\alpha^2x^8 + \dots$	$\alpha^6x^8 + \dots$	$\alpha^7x^{12} + \dots$
$f_2$	1			$\alpha^6x^8 + \dots$	$\alpha^7x^{12} + \dots$	$\alpha^2x^{12} + \dots$

which is a Gröbner basis with respect to  $>_{32}$ . In *Pairing* and *Voting* steps, the following data is computed:

$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_2$	1	$\alpha^3$
$f_1$	$g_0$	-3	$\alpha^3$
$f_2$	$g_1$	-3	$\alpha^3$

In *Rebasing* step, the pair  $f_0, g_2$  is modified by (17) while the pairs  $f_1, g_0$  and  $f_2, g_1$  are modified by (18). These modifications give the Gröbner basis with respect to  $>_{31}$ ,

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$						$x^9 + \dots$
$g_1$					$x^9 + \dots$	
$g_2$				$\alpha^7x^8 + \dots$	$\alpha^2x^8 + \dots$	$x^8 + \dots$
$f_0$			$x$	$2x^8 + \dots$	$\alpha^2x^9 + \dots$	$x^9 + \dots$
$f_1$		1		$\alpha^2x^8 + \dots$	$\alpha^6x^8 + \dots$	$2x^{11} + \dots$
$f_2$	1			$\alpha^6x^8 + \dots$	$2x^{11} + \dots$	$\alpha^2x^{12} + \dots$

After similar iterations, we eventually reach to the Gröbner basis with respect to  $>_{16}$  for  $v$ ,

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$						$x^9 + \dots$
$g_1$		$x + \dots$	$\alpha^7x^2 + \dots$	$2x^5 + \dots$	$x^7 + \dots$	$\alpha^7x^8 + \dots$
$g_2$			$x + \dots$	$\alpha^2x^7 + \dots$	$\alpha^5x^8 + \dots$	$x^9 + \dots$
$f_0$		1	$x^2 + \dots$			
$f_1$		$x^2 + \dots$	$\alpha^7x^3 + \dots$	$\alpha^7x^4 + \dots$	$\alpha^3x^6 + \dots$	$\alpha^7x^8 + \dots$
$f_2$	1	$\alpha^3x + \dots$	$\alpha^7x^2 + \dots$	$\alpha^3x^4 + \dots$	$\alpha^7x^6 + \dots$	$\alpha^3x^8 + \dots$

In *Pairing* and *Voting* steps, the following data is computed:

$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_1$	1	0
$f_1$	$g_2$	1	0
$f_2$	$g_0$	1	$\alpha^7$

Thus the value 0 gets 2 votes, and the value  $\alpha^7$  gets 1 vote. So  $w$  is set to be 0, and this result is recorded in  $w_{16} = 0$ . Then the pairs  $f_0, g_1$  and  $f_1, g_2$  are modified by (16). The pair  $f_2, g_0$  is modified by (17). Then we get the Gröbner basis with respect to  $>_{15}$  for  $v^{(15)} = v - \text{ev}(0 \cdot x^4y)$ ,

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$	1	$\alpha^3x + \dots$	$\alpha^7x^2 + \dots$	$\alpha^3x^4 + \dots$	$\alpha^7x^6 + \dots$	$\alpha^3x^8 + \dots$
$g_1$		$x + \dots$	$\alpha^7x^2 + \dots$	$2x^5 + \dots$	$x^7 + \dots$	$\alpha^7x^8 + \dots$
$g_2$			$x + \dots$	$\alpha^2x^7 + \dots$	$\alpha^5x^8 + \dots$	$x^9 + \dots$
$f_0$		1	$x^2 + \dots$			
$f_1$		$x^2 + \dots$	$\alpha^7x^3 + \dots$	$\alpha^7x^4 + \dots$	$\alpha^3x^6 + \dots$	$\alpha^7x^8 + \dots$
$f_2$	$x + \dots$	$\alpha^3x^2 + \dots$	$\alpha^7x^3 + \dots$	$\alpha^3x^5 + \dots$	$\alpha^7x^7 + \dots$	$\alpha^5x^8 + \dots$

In *Pairing* and *Voting* steps, we obtain

$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_0$	1	0
$f_1$	$g_1$	0	0
$f_2$	$g_2$	1	0

So  $w_{15} = w = 0$ . All three pairs  $f_0, g_0$ ,  $f_1, g_1$ , and  $f_2, g_2$  are modified by (16). Thus we get the Gröbner basis with respect to  $>_{14}$  for  $v^{(14)} = v^{(15)} - \text{ev}(0 \cdot x^5)$ ,

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$	1	$\alpha^3x + \dots$	$\alpha^7x^2 + \dots$	$\alpha^3x^4 + \dots$	$\alpha^7x^6 + \dots$	$\alpha^3x^8 + \dots$
$g_1$		$x + \dots$	$\alpha^7x^2 + \dots$	$2x^5 + \dots$	$x^7 + \dots$	$\alpha^7x^8 + \dots$
$g_2$			$x + \dots$	$\alpha^2x^7 + \dots$	$\alpha^5x^8 + \dots$	$x^9 + \dots$
$f_0$		1	$x^2 + \dots$			
$f_1$		$x^2 + \dots$	$\alpha^7x^3 + \dots$	$\alpha^7x^4 + \dots$	$\alpha^3x^6 + \dots$	$\alpha^7x^8 + \dots$
$f_2$	$x + \dots$	$\alpha^3x^2 + \dots$	$\alpha^7x^3 + \dots$	$\alpha^3x^5 + \dots$	$\alpha^7x^7 + \dots$	$\alpha^5x^8 + \dots$

Again *Pairing* and *Voting* steps result in

$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_2$	3	0
$f_1$	$g_0$	0	$\alpha^3$
$f_2$	$g_1$	0	$\alpha^3$

Note that the value 0 get 3 votes while the value  $\alpha^3$  get 0 votes. Thus  $w_{13} = w = 0$  is chosen. The pair  $f_0, g_2$  is modified by (16), and the pairs  $f_1, g_0$  and  $g_2, g_1$  are modified by (18). Thus the Gröbner basis with respect to  $>_{13}$  for  $v^{(13)} = v^{(14)} - \text{ev}(0 \cdot x^2y^2)$  is

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$	1	$\alpha^3x + \dots$	$\alpha^7x^2 + \dots$	$\alpha^3x^4 + \dots$	$\alpha^7x^6 + \dots$	$\alpha^3x^8 + \dots$
$g_1$		$x + \dots$	$\alpha^7x^2 + \dots$	$2x^5 + \dots$	$x^7 + \dots$	$\alpha^7x^8 + \dots$
$g_2$			$x + \dots$	$\alpha^2x^7 + \dots$	$\alpha^5x^8 + \dots$	$x^9 + \dots$
$f_0$		1	$x^2 + \dots$			
$f_1$	1	$x^2 + \dots$	$\alpha^7x^3 + \dots$			
$f_2$	$x + \dots$	$\alpha^3x^2 + \dots$	$\alpha^7x^3 + \dots$	$x^4 + \dots$	$2x^6 + \dots$	$x^8 + \dots$

From the result

$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_1$	2	0
$f_1$	$g_2$	2	0
$f_2$	$g_0$	0	2

we set  $w_{12} = 0$ , and the Gröbner basis with respect to  $>_{12}$  for  $v^{(12)} = v^{(13)} - \text{ev}(0 \cdot x^3y)$  is

	$y^2z$	$yz$	$z$	$y^2$	$y$	1
$g_0$	1	$\alpha^3x + \dots$	$\alpha^7x^2 + \dots$	$\alpha^3x^4 + \dots$	$\alpha^7x^6 + \dots$	$\alpha^3x^8 + \dots$
$g_1$		$x + \dots$	$\alpha^7x^2 + \dots$	$2x^5 + \dots$	$x^7 + \dots$	$\alpha^7x^8 + \dots$
$g_2$			$x + \dots$	$\alpha^2x^7 + \dots$	$\alpha^5x^8 + \dots$	$x^9 + \dots$
$f_0$		1	$x^2 + \dots$			
$f_1$	1	$x^2 + \dots$	$\alpha^7x^3 + \dots$			
$f_2$	$x + \dots$	$\alpha^3x^2 + \dots$	$\alpha^7x^3 + \dots$			

(20)

For every iteration from this point on,  $w_s = 0$  unanimously, and for the three gaps 5, 2, 1, there occurs no modifications. For brevity, we list only voting results:

$x^4$				$xy^2$				$x^2y$				$x^3$				$y^2$			
$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_0$	2	0	$f_0$	$g_2$	4	0	$f_0$	$g_1$	3	0	$f_0$	$g_0$	3	0	$f_0$	$g_2$	5	0
$f_1$	$g_1$	1	0	$f_1$	$g_0$	1	0	$f_1$	$g_2$	3	0	$f_1$	$g_1$	2	0	$f_1$	$g_0$	2	0
$f_2$	$g_2$	2	0	$f_2$	$g_1$	1	0	$f_2$	$g_0$	1	0	$f_2$	$g_2$	3	0	$f_2$	$g_1$	2	0

$xy$				$x^2$				$y$				$x$				$1$			
$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$	$f_i$	$g_{i'}$	$c_i$	$w_i$
$f_0$	$g_1$	4	0	$f_0$	$g_0$	4	0	$f_0$	$g_1$	5	0	$f_0$	$g_0$	5	0	$f_0$	$g_0$	6	0
$f_1$	$g_2$	4	0	$f_1$	$g_1$	3	0	$f_1$	$g_2$	5	0	$f_1$	$g_1$	4	0	$f_1$	$g_1$	5	0
$f_2$	$g_0$	2	0	$f_2$	$g_2$	4	0	$f_2$	$g_0$	3	0	$f_2$	$g_2$	5	0	$f_2$	$g_2$	6	0

Thus (20), with no modifications, remains as a Gröbner basis with respect to  $>_{-1}$ . Hence the recovered message is

$$(w_0, w_3, w_4, w_6, w_7, w_8, w_9, w_{10}, w_{11}, w_{12}, w_{13}, w_{14}, w_{15}, w_{16}) = 0 \in \mathbb{F}^{14}$$

and the recovered codeword is the zero codeword.

## V. FINAL REMARKS

We presented a unique decoding algorithm based on interpolation. Like the syndrome decoding algorithm, our decoding algorithm corrects errors of up to half of the order bound. It computes the message directly from the received vector under evaluation encoding, which is a distinctive feature of list decoding. Like Kötter's algorithm for syndrome decoding, our decoding algorithm is amenable to a parallel hardware architecture.

We would like to thank the anonymous referees for thoughtful comments that much improved the original paper.

## REFERENCES

- [1] T. Høholdt and R. Pellikaan, "On the decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1589–1614, 1995.
- [2] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, 1999.
- [3] K. Lee and M. E. O'Sullivan, "List decoding of Hermitian codes using Gröbner bases," *Journal of Symbolic Computation*, no. 44, pp. 1662–1675, 2009.
- [4] I. M. Duursma, "Majority coset decoding," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 1067–1070, 1993.
- [5] R. Kötter, "A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1353–1368, 1998.
- [6] W. Fulton, *Algebraic Curves*. Benjamin, 1969.
- [7] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed. Springer-Verlag, 2009.
- [8] E. Kunz, *Introduction to plane algebraic curves*. Birkhäuser, 2005.
- [9] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, ser. GTM. Springer-Verlag, New York, 1998, vol. 185.
- [10] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*. Perseus Books, 1969.
- [11] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, "A fast decoding method of AG codes from Miura-Kamiya curves  $C_{ab}$  up to half the Feng-Rao bound," *Finite Fields and Their Applications*, vol. 1, no. 1, pp. 83–101, 1995.
- [12] M. Bras-Amorós and M. E. O'Sullivan, "On semigroups generated by two consecutive integers and improved Hermitian codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2560–2566, 2007.
- [13] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry of codes," in *Handbook of coding theory, Vol. I, II*. Amsterdam: North-Holland, 1998, pp. 871–961.